APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/820,110	03/28/2001	Ramanathan Ramanathan	42390P10983	2329

			EXAMINER
8791	7590	02/11/2004	LAFORGIA, CHRISTIAN A

BLAKELY SOKOLOFF TAYLOR & ZAFMAN
12400 WILSHIRE BOULEVARD, SEVENTH FLOOR
LOS ANGELES, CA 90025

ART UNIT	PAPER NUMBER
2131	3

DATE MAILED: 02/11/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

	Application No.		Applicant(s)	
Office Action Summary	09/820,110		RAMANATHAN, RAMANATHAN	
	Examiner		Art Unit	
	Christian La Forgia		2131	

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _03 December 2001_.
2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.
3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is

closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-21_ is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-21_ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _28 March 2001_ is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage

        application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date _2_.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1 through 21 are presented for examination.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1 through 21 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent No. 6,253,322 to Susaki et al., hereinafter Susaki.

4. As per claims 1, 6, and 11, Susaki teaches a method comprising:

writing a party's authenticating information and a first digital certificate issuing authority's authenticating information in an electronic document (Figures 1 [blocks 122, 154, 160], 9a [block 1000a], 9b [block 1000b], 15 [blocks 2700, 2701]; column 2, line 57 to column 3, line 10; column 4, lines 33-57);

signing the electronic document to obtain a once signed electronic document (Figures 1 [blocks 161, 162], 9a [block 1001a], 9b [block 1001b], 15; column 2, line 57 to column 3, line 10; column 8, line 62 to column 9, line 19; column 12, lines 45-60); and

transmitting the once signed electronic document to a second digital certificate issuing authority to obtain a twice signed electronic document (Figures 1 [blocks 151, 152, 180], 9c [blocks 1001a, 1001b, 1001c]; column 2, line 57 to column 3, line 10; column 13, lines 11-52). The first signing is drawn to the self-certificate performed at a user's station and the transmitting

to the certificate authority (block 170 in Figure 1) is where the second signature is obtained for

the twice-signed electronic document. A further, more in depth, textbook explanation is given

on pages 34 through 41 of **Applied Cryptography Second Edition** by Bruce Schneier.

5.   Regarding claims 2, 7, and 12, Susaki teaches wherein signing the electronic document to

obtain a once signed electronic document comprises:

obtaining a hash value using contents of the electronic document as input to a hash

algorithm (Figures 6 [blocks 702, 704, 706], 10 [blocks 1105, 1106], 15; column 10, lines 35-58;

column 14, lines 1-38; column 19, lines 19-42);

encrypting the hash value using the first digital certificate issuing authority's private key

(Figures 6 [block 706], 15; column 10, lines 35-58; column 14, lines 1-38; column 19, lines 19-

42); and

storing the encrypted hash value in the electronic document (Figure 15 [block 2703];

column 19, lines 19-42).

6.   Regarding claims 3, 8 and 13, Susaki teaches wherein obtaining a twice signed electronic

document comprises at least one of

the second digital certificate issuing authority inserting its authenticating information in

the once signed electronic document (column 10, lines 47-58; column 12, lines 45-60),

obtaining a hash value using contents of the electronic document as input to a hash

algorithm (Figures 6 [blocks 702, 704, 706], 10 [blocks 1105, 1106], 15; column 10, lines 35-58;

column 14, lines 1-38; column 19, lines 19-42),

encrypting the hash value using the second digital certificate issuing authority's private

key, including the encrypted hash value in the electronic document (Figures 6 [blocks 702, 704,

706], 10 [blocks 1105, 1106], 15; column 10, lines 35-58; column 14, lines 1-38; column 19,

lines 19-42), and

transmitting the twice signed electronic document (column 13, lines 52-61).

7.   With regards to claims 4, 9, and 14, Susaki teaches wherein obtaining a hash value using

contents of the electronic document as input to a hash algorithm comprises at least one of:

using the party's authenticating information (column 8, line 62 to column 9, line 19),

using the first digital certificate issuing authority's authenticating information (column 8,

line 62 to column 9, line 19),

using the digital signature of the first digital certificate issuing authority (column 8, line

62 to column 9, line 19), and

using the second digital certificate issuing authority's authenticating information as input

to a hash algorithm (column 8, line 62 to column 9, line 19).

8.   Regarding claims 5, 10, and 15, Susaki teaches wherein writing a party's authenticating

information and a first digital certificate issuing authority's authenticating information in an

electronic document comprises receiving the party's authenticating information via a secure

connection (column 10, lines 34-58; column 11, lines 16-40).

9.   As per claims 16, 18, and 20, Susaki teaches a method comprising:

receiving a once signed electronic document (Figures 1 [blocks 151, 152, 180], 9c

[blocks 1001a, 1001b, 1001c]; column 2, line 57 to column 3, line 10; column 13, lines 11-52);

writing a digital certificate issuing authority's authenticating information in the once

signed electronic document (column 10, lines 47-58; column 12, lines 45-60);

signing the once signed electronic document to form a twice signed electronic document

(Figures 1 [blocks 151, 152, 180], 9c [blocks 1001a, 1001b, 1001c]; column 2, line 57 to column

3, line 10; column 10, lines 47-58; column 12, lines 45-60; column 13, lines 11-52); and

transmitting the twice signed electronic document (column 13, lines 52-61). The

receiving the first signed document is drawn to the certificate authority receiving the self-

certificate performed at a user's station (block 170 in Figure 1). The certificate authority is

where the second signature is obtained for the twice-signed electronic document. A further,

more in depth, textbook explanation is given on pages 34 through 41 of **Applied Cryptography**

Second Edition by Bruce Schneier.

10.   Regarding claims 17, 19, and 21, Susaki teaches wherein signing the once signed

electronic document to form a twice signed electronic document comprises:

obtaining a hash value using contents of the once signed electronic document and using

the digital certificate issuing authority's authenticating information as input to a hash algorithm

(Figures 6 [blocks 702, 704, 706], 10 [blocks 1105, 1106], 15; column 10, lines 35-58; column

14, lines 1-38; column 19, lines 19-42);

encrypting the hash value using the digital certificate issuing authority's private key

(Figures 6 [block 706], 15; column 10, lines 35-58; column 14, lines 1-38; column 19, lines 19-

42); and

writing the encrypted hash value in the electronic document (Figure 15 [block 2703];

column 19, lines 19-42).

Double Patenting

11.   The nonstatutory double patenting rejection is based on a judicially created doctrine

grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or

improper timewise extension of the "right to exclude" granted by a patent and to prevent possible

harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed.

Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686

F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA

1970); and, *In re Thorington,* 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

12.   A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to

overcome an actual or provisional rejection based on a nonstatutory double patenting ground

provided the conflicting application or patent is shown to be commonly owned with this

application. See 37 CFR 1.130(b).

13.   Effective January 1, 1994, a registered attorney or agent of record may sign a terminal

disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37

CFR 3.73(b).

14.   Claims 1 through 21 are provisionally rejected under the judicially created doctrine of

double patenting over claims 1, 4 through 8, 11 through 13, 16 through 19, 22, 23, 26, 27, and 30

of copending Application No. 09/945,913. This is a provisional double patenting rejection since

the conflicting claims have not yet been patented.

15.   The subject matter claimed in the instant application is fully disclosed in the referenced

copending application and would be covered by any patent granted on that copending application

since the referenced copending application and the instant application are claiming common

subject matter, as follows:

A method comprising:

writing a party's authenticating information and a first certificate issuing authority's

authenticating information in an electronic document;

signing the electronic document to obtain a once signed electronic document;

transmitting the once signed electronic document to a second digital certificate issuing

authority to obtain a twice signed electronic document.

16.   Furthermore, there is no apparent reason why applicant would be prevented from

presenting claims corresponding to those of the instant application in the other copending

application. See *In re Schneller*, 397 F.2d 350, 158 USPQ 210 (CCPA 1968). See also MPEP

§ 804.

Conclusion

17.   The prior art made of record and not relied upon is considered pertinent to applicant's

disclosure.

18.   The following patents are cited to further show the state of the art with respect to

certificate chaining, such as:

United States Patent No. 5,422,953 to Fischer, which is cited to show a method for inserting two certificates to ensure the validity of data.

United States Patent No. 6,615,350 to Schell et al., which is cited to show executable modules with several digital signatures in order to validate the data is correct.

United States Patent No. 5,497,422 to Tysen et al., which is cited to show ensuring messages by including a chain of certificates.

United States Patent No. 6,138,235 to Lipkin et al., which is cited to show code modules verified using digital certificates.

United States Patent No. 6,134,327 to Van Oorschot, which is cited to show a communications system with multiple certificate authorities for validating transmitted data.

United States Patent No. 6,370,249 to Van Oorschot, which is cited to show a communications system with multiple certificate authorities for validating transmitted data.

United States Patent No. 6,219,423 to Davis, which is cited to show a commonly assigned patent that illustrates a twice-signed document.

United States Patent No. 6,253,323 to Cox et al., which is cited to show a commonly assigned patent that illustrates a twice-signed document.

United States Patent No. 5,825,880 to Sudia et al., which is cited to show a method for using several certificate authorities to create a signed document.

United States Patent No. 6,209,091 to Sudia et al., which is cited to show a method for using several certificate authorities to create a signed document.

United States Patent No. 6,367,013 to Bisbee et al., which is cited to show a method for inserting two certificates to ensure the validity of data with regards to time.

United States Patent No. 5,659,616 to Sudia, which is cited to show a method for using digital signatures in a commercial cryptographic system.

United States Patent No. 5,465,299 to Matsumoto et al., which is cited to show an electronic document processing system.

19.   Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian La Forgia whose telephone number is (703) 305-7704. The examiner can normally be reached on Monday thru Thursday 7-5.

20.   If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (703) 305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

21.   Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Christian LaForgia
Patent Examiner
Art Unit 2131
Clf

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100